UNREDACTED VERSION OF EXHIBIT 18 SOUGHT TO BE FILED UNDER SEAL

From: "Thomas E. Gorman" <TGorman@kvn.com>
To: Kristinn Gudjonsson [redacted]>
Cc: Brian Ferrall <BFerrall@KVN.com>, Shana Stanton [redacted], "Raquel Small ([redacted]
Subject: RE: MAC address question
Sent: Thu, 23 Feb 2017 01:22:27 +0000

So, he wiped it / re-imaged it on 2015-10-16?
Can we crack it now that you found this record of a key-escrow message?
--Tom

From: Kristinn Gudjonsson [mailto[redacted]
Sent: Wednesday, February 22, 2017 4:31 PM
To: Thomas E. Gorman
Cc: Brian Ferrall; Shana Stanton; Raquel Small[redacted]
Subject: Re: MAC address question

Hi

Just a quick update to this thread. There were quite a few discrepancies in both theories that were ongoing, the two hypothesis that I was working with were:

1. Hard disk didn't get swapped, the machine got re-imaged on 2015-10-16 and both our inventory system and [redacted]
2. Anthony swapped the drives and installed another system on the machine

I started asking around about the possibilities of nr. 1 but I got such an assurance from many people that it couldn't happen so I started pursuing the second theory. Which at first started to pan out and start looking very promising. However once I started digging further most of the evidence I got to piece together (see the timeline) seemed to suggest that this could in fact be "legit".

Therefore in the last few days I've been pursuing hypothesis 1. And in doing so I've discovered several things that support that theory:

1. Timeline matches nicely, from time of drive re-formatting to when we see traffic coming from the machine
2. Looking at collected syslogs from the machine it does indicate that [redacted]
3. Looking at the encrypted image that i've got I noticed two things, a)[redacted]
4. There were also quite a few misconfigurations on the machine, starting with the fact that it got re-imaged as a Desktop role, which would lead to several failures. Also the machine never successfully ran our Goobuntu updater, which could result in some of the values that we are seeing not getting synced in.

I'm still running down few things to confirm things, but it is starting to look like that because Anthony re-imaged the machine as a desktop role and not as a laptop that few things started to fail. Also it is starting to look like the image that I've got is in fact the drive that was running on the drive, that there is probably no mystery drive.

I still don't have good answers of WHY[redacted]d, few questions that are outstanding there before I can confirm this hypothesis though. Also ... the serial number for the hard drive is still plaguing me..[redacted] DOES indicate that the drive that got collected is in fact the one running the corporate image BUT at the same time it reports the original serial number.

The fact that the serial number is "wrong" in our inventory system could be explained by the fact that the updater never ran successfully, however it does not explain the fact that the encryption config showed the wrong serial number. So I still need to confirm why that is the case.... one reason is that the actual hard drive reports different serial number than the one on the sticker. I've asked Thomas to ask Discovia to tell me the reported serial number from the drive to confirm that hypothesis.

So basically the TL/DR (hidden at the end of the message) is that it is starting to look like a mixture of failures in our inventory[redacted] and bad configuration of the host (using desktop role) that lead to these discrepancies and not a disk swapping.

I've updated the tracking doc to reflect the current standing of the outcome and will remove the disclaimers once I actually get answers to the rest of my questions.

On Fri, Feb 17, 2017 at 3:38 PM Thomas E. Gorman <TGorman@kvn.com> wrote:

He sent in his resignation letter late on 1/26, so he knew the night before. (To be honest, he was planning his exit for weeks—maybe months—but he hadn't picked a date until the last minute.)
He was exited mid-morning on 1/27. He had one exit interview that day with Chelsea, and he was walked out of the building. He came back for a follow-up exit interview (at his request) on 2/1.
These dates are all verified with cross-checked interviews, contemporaneous emails, and contemporaneous notes.

What is NOT verified is the collection of his devices. As far as I know, we have yet to receive a precise tick-tock from Chelsea's team on when they grabbed the computers. (Was it on 1/27? Later that week? Did Anthony bring in a device on 2/1? It's very). I think that they've checked their notes and emails, but I get the impression that they didn't take note of when they took custody of the devices. But you've probably talked to them more than I have at this point. If they have not been responsive, please let us know, because Shana and Raquel can help us on that front.
--Tom

From: Kristinn Gudjonsson [redacted]
Date: Friday, February 17, 2017 at 1:38 PM
To: Thomas Gorman <TGorman@kvn.com>
Cc: Brian Ferrall <BFerrall@KVN.com>, Shana Stanton [redacted] Raquel Small [redacted]
Subject: Re: MAC address question

Quick questions for you.

When was the exit interview? as in do you have accurate timestamps of that? And when did he know that he was being let go, was that just at the same time as the exit interview or a day ahead, or...

On Fri, Feb 17, 2017 at 12:22 PM Kristinn Gudjonsson <[redacted]> wrote:
Hi

So... it is starting to look like the computer was not collected at the time of exit, both because we still see network activity from it after the exit, which would indicate it was turned on and also because the HRBP and person that delivered the machines does not recollect collecting two laptops during the exit interview.

However, what I can tell you is that [redacted] There is no way he could have copied the data over to a new drive and put his work stuff on the Replacement HD and continued to work from that. That would have been reported through our chain of inventory systems, since [redacted]

And the timeline also matches, the computer was plugged into Ethernet, called out for an IP address, did not provide any hostname and then got turned down, few minutes later it is turned back on and this time it starts sending out syslog messages that are indicative of a computer boot sequence (not sleep mode, but boot). This indicates that we have a Assigned HD back inserted into the computer.

I have not yet seen any signs that this Replacement HD was ever put back into the computer, except for the last time it got mounted, which is still January 26th... so I'm still trying to double check and answer why that date is there and how that fits the puzzle, since we still see syslogs being collected from the Assigned HD after that date.

So I don't have all the answers yet, but this is starting to come together.

On Fri, Feb 17, 2017 at 11:54 AM Thomas E. Gorman <TGorman@kvn.com> wrote:
ATTORNEY WORK PRODUCT PRIVILEGED
(- David & Ed @ KVN)
(+ Shana and Raquel @ Google Legal)
Kristinn—
This explanation does help a great deal. Thank you.
First, I'm not doubting your conclusions but something seems off here. I don't know enough about ho[redacted] so I can't quite but my finger on it, but I'm inclined to push back just b/c of Occam's Razor.
You confirmed that the Replacement HD was installed on 10-26-2015. And you pulled the Replacement HD out of the laptop on 02-17-2016. The simplest explanation is that the Replacement HD was in that computer for that entire period. The second simplest explanation is that someone swapped the drive into the computer in January/February b/c he/she didn't realize that the computer

was supposed to be preserved. (In particular, the data that you have showing [redacted]pings every hour doesn't reconcile with the drive being collected on 1/27, so maybe this laptop was sitting on his desk for a couple weeks, and IT tried to repurpose it?).

Put simply, this is a pretty complicated way to hide evidence. Why not wipe the drive (like he did with the other laptop)? Or just throw the laptop into the Bay? Sending someone to sneak in—after Anthony was terminated—to swap drives is really sinister.

If we can prove that that's what happened, then let's pursue that aggressively. I just want to make sure that you rigorously double check all the less-sinister possibilities. We don't want include these allegations in a legal proceeding if they may not hold up.

Please let me know if you have any questions, or would like to discuss further.

Thanks

--Tom

From: Kristinn Gudjonsson [mailto:[redacted]]
Sent: Thursday, February 16, 2017 6:17 PM
To: Thomas E. Gorman
Cc: Brian Ferrall; David W. Rizk; Edward A. Bayley
Subject: Re: MAC address question

Hi

... and then let's start with attempting to answer the more complicate questions...

And yes, the wording may have complicated things a bit... the wording of "corp image", "corp" this or that refers to the assigned HD. That is the drive that came with the machine, Goobuntu was installed on and has corporate access (hence corp references).

I did not say that the replacement drive was first inserted into the computer on 2015-10-26, that I do not know. What i do know is that is the time an encrypted Ubuntu OS was installed on that particular hard drive. It could have been that the Replacement HD was inserted there before and running a different OS version. But at that date it seems as the OS was setup. And it was not Goobuntu, since if it was Goobuntu that was installed on the Replacement HD then we would have seen records of that in our inventory system...

Then shortly after that (few minutes later) the hard drives were swapped since that same computer comes up again, this time running the Assigned HD version.

What happens later I've not completely answered, that is I have not mapped up the entire time between October of 2015 until February of 2016, it could well have been that the drives were swapped sometime during that timeframe. However what I do know is that the Assigned HD was running on the machine until 2016-01-31, since we have both [redacted] records with the assigned hostname of anthonyl-glaptop as well as logs collected from the machine, all pointing to the Assigned HD, as well as our inventory system seeing the system live and collecting the serial number of the drive.

What I also know is that what we got delivered to us was not the Assigned HD but the Replacement one. So sometime between 01/31 and 02/17 when I get the device in my hand that the Assigned HD is removed and the Replacement one is put in it's place. And most likely that happens on 02/03, since that is the last time our inventory systems see it alive.

Does that answer some of the confusion?

On Thu, Feb 16, 2017, 18:08 Kristinn Gudjonsson <[redacted]> wrote:

Let's start answering the easy questions...

YEs I still have the shells, or the actual laptops in our lab.

And no I don't have a chain of custody documentation. Unfortunately that was not started for this case.

On Thu, Feb 16, 2017, 16:55 Thomas E. Gorman <TGorman@kvn.com> wrote:

Easy questions first:

Also, do you still have the laptops (minus the hard drives) in SecOps?

And do you have documentation on the chain of custody for those? Google Legal is asking me.

From: Kristinn Gudjonsson [mailto:[redacted]]
Sent: Thursday, February 16, 2017 3:07 PM

To: Thomas E. Gorman
Cc: David W. Rizk; Brian Ferrall; Edward A. Bayley
Subject: Re: MAC address question

Hi

So I'm starting to move away from the theory of the lab machine. Digging further into this it seems like Anthony may have swapped the hard drives on 2015-10-16, installed a Goobuntu on the hard drive that got returned, and then swapped drives again.

I can see the following timestamps from various sources (all in PST8PDT) and all on 2015-10-26:

- 14:26:23 [redacted] request coming from the ethernet port of the Thinkpad machine, an IP address of [redacted] is issued
- 14:26:57 the folder /lost+found is created on the unencrypted partition of the drive. This indicates the creation time or around that fo[redacted]
- 14:41:01 the last time the [redacted] is modified.
- 14:47:06 - anthonyl-glaptop is booted using the corp image.
- 15:06:13 a [redacted] request is made from the WIFI card of the Thinkpad, and the hostname of anthonyl-glaptop is advertised

So reading through this timeline it looks like the hard drive of the machine was removed and swapped with the drive that got returned to us. Then the installation of the OS proceeded and the drive got encrypted, the final steps of that ncryption is to create the bootstrapping partition, which results in the timestamps listed above. Ubuntu uses LVM for handling logical volumes and names the volumes using the following pattern HOSTNAME-vg-MOUNTPOINT, so eg. anthonyl-glaptop-vg-root or something similar. In the case of the encrypted machine that we received there was no hostname associated to the host, in which case the IP address is used instead, and that was [redacted]. So I looked at [redacted] allocations coming from that time, and saw that it came from the ethernet port of anthonyl-glaptop.

So it looks like he or someone else with physical possession of the his computer swapped drives, installed Ubuntu on the machine, encrypted it, and then switched drives again and used the corp drive.

This is happening at the time of installation/creation of that drive.

What we then know is that the corp hard drive is still active after Anthony is exited, since we see records until 2016-01-31 18:15:10.282674 UTC or 2016-01-31 10:15 PST from the corp machine.

I'm still trying to determine at what time the drive could have been swapped. That could have been at this point anytime from the 31st until time of collection, which is most likely 02/03.

On Wed, Feb 15, 2017 at 4:29 PM Thomas E. Gorman <TGorman@kvn.com> wrote:

(+KVN team)
That was my next question.
The Loon lab tech ought to account for all six of those laptops (and all six of those hard drives).
Can you put a time stamp on when the drive might have been swapped?
--Tom

From: Kristinn Gudjonsson [mailto[redacted]
Sent: Wednesday, February 15, 2017 4:26 PM
To: Thomas E. Gorman
Subject: Re: MAC address question

And I'm going to follow up with the person responsible for that lab to ask if they noticed one machine breaking down or missing a hard drive

On Wed, Feb 15, 2017, 16:22 Kristinn Gudjonsson [redacted] wrote:

... and Chelsea is tracking down the person that did the collection, however they both transferred teams and it also looks like they are on paternity leave ATM.

On Wed, Feb 15, 2017 at 4:21 PM Kristinn Gudjonsson [redacted] wrote:
What I see is that the [redacted] shows that it had a particular IP address. [redacted] logs for that IP address show a MAC address... that MAC address belongs to this particular hardware, that was used in the Loon hardware lab at the time of the disk swapping...

On Wed, Feb 15, 2017 at 4:18 PM Kristinn Gudjonsson [redacted] > wrote:
I believe I may have located from what machine this hard drive came from.

There were six test machine ordered for testing in RLS1, these were ordered by the Loon team, refurbished old laptops. They were to be run using standard Ubuntu, not corp images and were plugged into RLS1's network., the purpose:

"""
We use these in our Loon hardware development lab - need the flexibility and portability of laptops, but need flexible, multi-user logins
"""

This machine then later got refurbished again and put on corp, that's why I got the MAC address of it associated to this particular machine. My hypothesis, someone knew they were about to collect Anthony's machine and they went inside the Loon hardware development lab, grabbed the hard drive from one of the test machines there and slapped it into the one that Anthony had... and then returned the laptop to HRBP.....

On Wed, Feb 15, 2017 at 3:35 PM Kristinn Gudjonsson [redacted] wrote:
So... what I've got now is by looking at [redacted] we got.
In order to boot your machine you need to [redacted]

[redacted]

That tells me that this is an Ubuntu setup, which does not run any internal builds and has never been registered in our inventory systems. It also was plugged into the wall at RLS1 into the [redacted], again meaning this was not a machine with corporate credentials on it.

And this was not the hard drive that was in anthonyl-glaptop...

Chelsea is still looking at her notes, etc... the person that did the collection has since moved to a different team and we are trying to get a hold of them.

On Wed, Feb 15, 2017 at 3:19 PM Kristinn Gudjonsson [redacted] wrote:
Hi

I'm chasing down few leads right now... but [redacted].. thus we are pretty sure about the serial number.... this hard drive has never been on a machine that is in our inventory system.....

On Wed, Feb 15, 2017 at 1:51 PM Thomas E. Gorman <TGorman@kvn.com> wrote:
Since we're going down a rabbit hole based on the [redacted] logs, how sure are you that the MAC address in those logs is ***actually*** the MAC address for anthonyl-glaptop?
I only ask b/c of the discrepancy with the drive S/N. Maybe the problem is in that inventory system (i.e. it has the wrong drive S/N, and the wrong MAC address).
Something to think about anyway.
--Tom

--

with regards

Kristinn

--

with regards

Kristinn

--

with regards

Kristinn

--

with regards

Kristinn

--

with regards

Kristinn

--

with regards

Kristinn

--

with regards

Kristinn

--

with regards

Kristinn

--

with regards

Kristinn

--

with regards

Kristinn

--

with regards

Kristinn